CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION

J6 | CJCSI 8010.01
DISTRIBUTION: A, B, C, J, S | 7 July 2000

JOINT COMMUNITY CHIEF INFORMATION OFFICER

References: See Enclosure B.

1. Purpose. This instruction assigns the position of Joint Community (JC) Chief Information Officer (CIO), establishes applicable policy, and outlines the duties and responsibilities of that position.

2. Cancellation. None.

3. Applicability. This instruction applies to the Joint Staff, combatant commands, and other joint activities that are responsible to the Chairman of the Joint Chiefs of Staff.

4. Policy

a. The Director, Command, Control, Communications, and Computer Systems Directorate, J-6, Joint Staff, is designated the JC CIO with duties and responsibilities as described herein.

b. Director, Joint Staff, retains the responsibilities of the Joint Staff CIO. Details of these responsibilities are found in JSI 8000.01.

c. Director for Intelligence, J-2, Joint Staff will represent the JC at the Intelligence Community Chief Information Officer (IC CIO) Executive Council for intelligence and intelligence-related National Security Systems (NSS).

d. Combatant commands will designate a CIO and develop appropriate guidance for their area of responsibility. The CINC CIO's will normally use the JC CIO as their conduit to the DOD CIO and Executive Board, but have the latitude to directly contact the DOD CIO when desired. CINC CIOs will normally use the J-2 as the conduit for issues of intelligence and intelligence-related NSS to the IC CIO Executive Council.

e. Joint Staff directorates will normally use the JC CIO as a conduit to the DOD CIO Executive Board or J-2 for access to the IC CIO Executive Council on issues that involve their functional area and affect the JC. J-2 will coordinate with J-6 as Joint Community CIO on intelligence systems that impact or interact with operational systems.

f. The JC and CINC CIOs will assist the DOD and Service CIOs in fulfilling their mandated responsibilities. (See Enclosure A.)

5. Definitions. Refer to the Glossary.

6. Responsibilities. The JC CIO:

a. Provides advice and assistance to Joint Staff Senior Management and CINC CIOs on issues pertaining to information technology (IT) and NSS.

b. Coordinates with J-2 on intelligence and intelligence-related NSS issues (reference l).

c. Provides direct or indirect support to efforts to define, revise, or extend IT architectures that affect the JC and future joint operational and security requirements.

d. Supports CINCs on policy and capital investment issues external to the Joint Staff.

e. Supports requirements of both the Joint Requirements Oversight Council (JROC) and DOD CIO to determine compliance of interoperability standards by reviewing the interoperability key performance parameters (KPP) of Capstone requirements documents (CRD) and operational requirements documents (ORD) required by CJCSI 3170.01 and 6212.01.

f. Coordinates proposed architectures, policies, guidance, instructions, and directives from the DOD CIO with the Joint Staff and CINCs, then prepares a consolidated joint position.

g. Reviews IT and NSS efforts to ensure programs are not duplicative and are consistent with the Global Information Grid (GIG) architecture.

h. Assists the DOD CIO in the development and implementation of sound information assurance policies and guidance.

i. Advocates the development and priority of joint IT systems to the DOD CIO, CINCs, Services, and DOD agencies.

j. Represents the Joint Community as a whole at Federal and interagency bodies supporting IT policies; i.e., the CIO Executive Board and Architecture Coordination Council. The JC CIO will assist J-2 on national IC bodies supporting IT policies. Provides feedback to JC on issues they forward to these Federal and interagency bodies.

k. Serves as the entry point on the Joint Staff for Military Department CIOs' compliance with 10 USC Section 2223. The JC CIO coordinates with all other Joint Staff directorates on these IT and NSS.

l. Establishes an overarching JC CIO Council responsible for collaboration, management, and integration of cross-cutting issues, including information management, information resource management, strategic plans, and the Information Technology Capital Investment Portfolio. Membership is composed of representatives from the CINCs and Joint Staff directorates.

m. Resolves issues involving NSS. Certain portions of the Clinger-Cohen Act (C-CA) apply to NSS while others are to be "applied to the extent practicable." JC CIO recognizes the potential benefit the C-CA process mandates across NSS areas, as long as joint requirements maintain their priority, and are always met or exceeded. If an IT/NSS issue arises within the JC that necessitates the intervention of a mediator, it will first be coordinated with the JC CIO. The JC CIO will, in turn, represent the joint requirement to the DOD CIO for final disposition. For issues involving intelligence and intelligence-related NSS, J-2 will present these issues at the IC CIO Executive Committee.

7. Summary of Changes. None.

8. Releasability. This instruction is approved for public release; distribution is unlimited. DOD components (to include the combatant commands), other Federal agencies, and the public may obtain copies of this instruction through the Internet from the CJCS Directives Home Page--http://www.dtic.mil/doctrine/jel/cjcsd.htm. Copies are also available through the Government Printing Office on the Joint Electronic Library CD-ROM.

9. Effective Date. This instruction is effective upon receipt.

For the Chairman of the Joint Chiefs of Staff:

C.W.

C.W. FULFORD, JR.
Lieutenant General, U.S. Marine Corps
Director, Joint Staff

Enclosures:
A -- Summary of Responsibilities for the Department of Defense and Service Chief Information Officers
B -- References
Glossary

DISTRIBUTION

Distribution A, B, C, J, and S plus the following:

	Copies
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)	4
Director, Central Intelligence Agency	2
Director, National Security Agency	2
Director, Defense Information Systems Agency	2
Director, General Services Administration	2

(INTENTIONALLY BLANK)

ENCLOSURE A

SUMMARY OF RESPONSIBILITIES FOR THE DEPARTMENT OF DEFENSE AND SERVICE CHIEF INFORMATION OFFICERS

1. Advise and assist the head of the executive agency and senior management on IT.

2. Ensure IT is acquired and its resources managed in accordance with the C-CA.

3. Develop, maintain, and facilitate the implementation of a sound and integrated IT architecture.

4. Promote effective and efficient design and operation of all major information resource management (IRM) processes.

5. Monitor the performance of IT programs, evaluate them based on performance measures, provide advice on the continuation, modification, or termination of programs.

6. Assess requirements for department personnel regarding knowledge and skills to facilitate achievement of performance goals for IRM.

7. Assess the extent to which current personnel meet the knowledge and skill requirements.

8. Develop strategies for hiring, training, and professional development of personnel to meet knowledge and skills requirements.

9. Advise department heads on design, development, and implementation of information systems.

10. Review and provide recommendations on department budget requests for IT and NSS.

11. Ensure interoperability of IT and NSS.

12. Prescribe IT and NSS standards that apply throughout the department.

13. Provide for elimination of duplicate IT and NSS within the Military Departments and Defense agencies.

14. Design and implement a process for maximizing the value and assessing and managing the risk of department IT acquisition.

15. Institutionalize performance-based and results-based management for IT in coordination with the Chief Financial Officer.

16. Ensure information security policies, procedures, and practices are adequate.

17. Oversee contracts that provide for multiagency acquisition of IT.

18. Identify major IT acquisition programs that have significantly deviated from costs, performance, or schedule goals.

19. Develop a strategic plan that addresses the management and use of IT capabilities and provides overall direction and guidance for managing information resources.

20. Chair the department CIO Executive Board.

ENCLOSURE B

REFERENCES

a. 40 USC Chapter 25, Sections 1401-1503 (aka Clinger-Cohen Act of 1996 and Information Technology Management Reform Act (ITMRA))

b. 44 USC Chapter 35, Sections 3501-3520 (Paperwork Reduction Act of 1995)

c. 10 USC Chapter 131, Section 2223 (aka Strom Thurmond Act)

d. Executive Order 13011, Federal Information Technology

e. Secretary of Defense Memorandum, 2 June 1997, "Implementation of Subdivision E of the Clinger-Cohen Act of 1996 (Public Law 104-106)"

f. Office of Management and Budget Circular A-130, 8 February 1996, "Management of Information Resources"

g. Government Performance and Results Act (GPRA) of 1993, (Public Law 103-62)

h. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, 10 August 1999, "Requirements Generations System"

i. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01B, 8 May 2000, "Interoperability and Supportability of National Security Systems and Information Technology Systems"

j. DOD Information Management (IM) Strategic Plan, 19 October 1999

k. Joint Staff Instruction (JSI) 8000.01, 7 December 1995, "Information Resource Management Program"

l. DCI Directive 1/6, 4 February 2000, "Intelligence Community Chief Information Officer, Intelligence Community Chief Information Officer Executive Council, Intelligence Community Chief Information Officer Working Council"

m. CJCSI 5132.01, 2 May 1997, "Joint Requirements Oversight Council (JROC) Charter"

n. DOD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 8-8001, 31 March 2000, "Global Information Grid"

(INTENTIONALLY BLANK)

GLOSSARY

PART I--ABBREVIATIONS AND ACRONYMS

CRD	Capstone requirements document
GIG	Global Information Grid
IM	information management
IRM	information resource management
IS	information system
IT	information technology
ITCIP	Information Technology Capital Investment Portfolio
JROC	Joint Requirements Oversight Council
KPP	key performance parameters
NSS	National Security Systems
ORD	operational requirements document

PART II--DEFINITIONS

Capstone requirements document. A document that contains capabilities-based requirements that facilitates the development of individual ORDs by providing a common framework and operational concept to guide their development. It is an oversight tool for overarching requirements for a system-of-systems or family-of-systems.

combatant command. A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities.

Global Information Grid. The globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating and managing information on demand to warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services and other associated services necessary to achieve information superiority. It also includes NSS as defined in section 5142 of the Clinger-Cohen Act of 1996. The GIG supports all Department of Defense, National Security, and related-intelligence community missions and functions (strategic, operational, tactical and business) in war and in peace. The GIG provides capabilities from all operating locations (bases, posts, camps, stations, facilities, mobile platforms, and deployed sites). The GIG provides interfaces to coalition, allied, and non-DOD users and systems.

information assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. (DODD S-3600.1)

information management. The planning, budgeting, collecting, collating, correlating, manipulating, fusing, storing, archiving, retrieving, controlling, disseminating, protecting, and destroying of information throughout its life cycle.

information resource management. The process of managing information resources to accomplish agency missions and to improve agency performance. The term encompasses both information and the related resources such as personnel, equipment, funds, and information technology.

information system. (1) A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44USC 3502(8). (2) The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In addition, the hardware, software, and personnel associated with a system or system-of-systems that processes information to accomplish a function (DCI Directive 1/6).

information technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. This includes equipment used by a component directly or used by a contractor under a contract with the component that (1) requires the use of such equipment, or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term also includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. Notwithstanding the above, the term does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Information Technology Capital Investment Portfolio. An investment governance mechanism that supports the Department of Defense's implementation of the Clinger-Cohen Act of 1996, Division E, and other laws, policies, and guidance for managing IT investments. The ITCIP is intended to provide the CIO with better information to support management and investment decisions; to assist functional managers to effectively build and manage IT portfolios to fulfill strategic visions, goals, and related measures of performance; and to assist program managers to effectively manage performance, cost, and schedule risks in the acquisition of IT.

joint community. The directorates on the Joint Staff, combatant commands, and joint activities that are responsible to the Chairman of the Joint Chiefs of Staff.

Joint Requirements Oversight Council. Senior advisory council to the Chairman of the Joint Chiefs of Staff that assists in identifying and assessing the priority of joint military requirements, assessing warfighting capabilities, evaluating alternatives to any acquisition program, assigning priority among existing and future major programs, reviewing major warfighting deficiencies that require major acquisition programs, and resolving cross-Service requirement issues.

key performance parameters. Those capabilities or characteristics considered most essential for successful mission accomplishment. Failure to meet an ORD KPP threshold can be cause for the concept of system selection to be reevaluated or the program to be reassessed or terminated. Failure to meet a CRD KPP threshold can be cause for the family-of-systems or system-of-systems concept to be reassessed or the contributions of the individual systems to be reassessed. KPPs are validated by the JROC.

National Security Systems. Any telecommunications or information system operated by the USG, the function, operation, or use of (1) involves intelligence activities, (2) involves cryptologic activities related to national security, (3) involves command and control of military forces, (4) involves equipment that is an integral part of a weapon or weapons system, or (5) is critical to the direct fulfillment of military or intelligence missions. They do not include systems that are to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

operational requirements document. A formatted statement containing performance and related operational parameters for the proposed concept or system. Prepared by the user or user's representative at each Milestone beginning with Milestone I.